

REMARKS

Claims 1-3, 5-7 and 9-13 are pending. By this Amendment, claims 1, 3, 5-7 and 9-13 are amended. Support for these amendments may be found on p. 23, line 12 - p. 24, line 17; p. 23, lines 20-22; Figs. 3 and 4 and in the original and/or previously presented claims 1-3, 5-7 and 9-13, for example. No new matter is added.

Applicant appreciates the courtesies extended to Applicant's representatives Kip Werking and Daniel Tucker during the January 8, 2007 personal interview. The substance of the personal interview is incorporated into the Remarks below.

As discussed during the personal interview, claims 1 and 5 have been amended to recite "performing itself"; claims 3, 6 and 7 as well as 9, 11 and 12 have been amended to recite "independent of the connection server"; and claims 10 and 13 have been amended to recite "wait state in which the connection server allows communication from the address of the client apparatus." Although Applicant respectfully asserts that these amendments are not necessary to place the application in condition for allowance, the amendments are made to further prosecution.

I. Claim Rejections under 35 U.S.C. §112, second paragraph

The Office Action rejects claims 1-3, 5-7 and 9-13 under 35 U.S.C. §112, second paragraph. This rejection is respectfully traversed.

Applicant appreciates the indication in the Advisory Action that the rejections of the claims under 35 U.S.C. §112, second paragraph, regarding the terms "associating" and "predetermined method" have been withdrawn. However, the Advisory Action also indicates that the remaining rejections under 35 U.S.C. §112, second paragraph, have been maintained "due to the lack of clarity over what appears to be a first authentication performed by one

apparatus, and a second authentication performed by another different apparatus at a later point in time."

Regarding the remaining rejections under 35 U.S.C. §112, second paragraph,

Applicant respectfully submits that:

- A. the responses to two of these rejections are further explained for the purpose of clarity;
- B. the responses to five of the remaining rejections already explained the differences between the two authentication processes and so the responses to these rejections are repeated verbatim; and
- C. all of the other remaining rejections do not relate to a first authentication process performed by one apparatus and a second authentication performed by another apparatus and so the responses to these rejections are repeated verbatim.

A. The responses to two of the remaining rejections are further explained for the purpose of clarity

Regarding claims 1 and 2, the Office Action asserts that the limitation reciting a sixth unit is confusing as to whether the first connection authentication information is received from the client address or the authentication server. Claim 1 is amended for the purpose of clarity. Applicant respectfully submits that the first connection authentication information is received from the client address after such reception is allowed by the connection server. See Fig. 4, for example.

Regarding claim 6, the Office Action asserts that the limitation which recites "generated by encrypting using a second encryption method" is indefinite as to whether the "input by the user" is the same set of input used for the "first encrypted user name and first encrypted password." However, Applicant respectfully submits that the claim recites that the second encrypted name and second encrypted password are generated by encrypting using a second encryption method a user name and password input by the user. Thus, the input by the

user need not be the same as the input used for the "first encrypted user name and first encrypted password".

B. The responses to five of the remaining rejections already explained the differences between the two authentication processes

Regarding claim 5, the Office Action asserts that this claim is unclear as it appears that both the connection server authentication unit and the authentication server receive the same information to perform an authentication process. However, Applicant respectfully submits that both the connection server authentication unit and the authentication server receive authentication information from the client and perform an authentication process with the respective pieces of information. These component perform their respect authentication processes at different stages of operating the network connection system. The authentication server performs an authentication process when it first receives a connection request from the client. See p. 25, lines 8-19, for example. The connection server performs an authentication process later, after allowing the client to communicate. See p. 26, line 17 - p. 27, line 23. Furthermore, claim 5 does not recite that the respective pieces of authentication information must be the same.

Regarding claims 6, 9 and 13, the Office Action asserts that the claim is indefinite as to whether the first encryption method and the second encryption may be the same. However, Applicant respectfully submits that they may be the same. See p. 28, lines 3-5, for example.

Regarding claim 12, the Office Action asserts that the limitation reciting second connection authentication information is indefinite as to whether first and second authentication information are the same. However, Applicant respectfully submits that the first authentication information is the unique information. Furthermore, the second authentication information is the user name and password. Applicant notes that claim 12

does not recite first authentication information or second authentication information but does recite first and connection authentication information. The first connection authentication information is the same as the second authentication information (e.g. the user name and password). See p. 23, lines 20 - p. 24, line 2, for example.

Regarding claim 12, the Office Action asserts that the limitation which begins "transmitting the client address" is indefinite as to how the user identification information is authenticated based on the second connection authentication information. However, Applicant respectfully submit that the user identification information is the encrypted username and password sent to the authentication server by the client. After receiving the user identification information, the authentication server checks to see if the same information, as second connection authentication information, is stored in the authentication server's memory. See p. 25, lines 8-19, for example.

Regarding claims 12 and 13, the Office Action asserts that the claim is indefinite with respect to which component of the apparatus performs various steps. However, Applicant respectfully submits that claims 12 and 13 are method claims and, as such, do not require further structural limitations.

C. All of the other remaining rejections do not relate to a first authentication process performed by one apparatus and a second authentication performed by another apparatus

The Office Action asserts that the claims are generally narrative and indefinite, failing to conform with U.S. practice. Applicant respectfully disagrees.

The claims properly recite a combination of elements and the functions they perform. This does not render the claims narrative or indefinite and is completely consistent with U.S. practice. As stated in MPEP 2114 and 2173.05(g), "features of an apparatus may be recited

structurally or functionally" and "there is nothing inherently wrong with defining some part of an invention in functional terms," respectively. Accordingly, the form and style of the claims are not narrative, indefinite or failing to conform to U.S. practice based on functional limitations.

Regarding claims 1 and 2, the Office Action asserts that two limitations contradict each other because they recite that the second connection authentication information is generated by two different components (the client apparatus and the connection server). Applicant respectfully submits, however, that these limitations do not contradict each other but only correspond to different stages of using the apparatus. The connection server generates the second connection authentication information during the setup stage. See p. 22, line 22 - p. 23, line 2, for example. The client apparatus generates the second connection authentication information during the authentication processing stage. See p. 23, line 12 - p. 24, line 8, for example.

Regarding claim 6, the Office Action asserts that the limitation reciting a retention unit is unclear as to whether the first encrypted user name and first encrypted password are a first encrypted user name and password and/or a set of user name and password encrypted by a first encryption method. However, Applicant respectfully submits that the first encrypted user name and first encrypted password are a set of user name and password encrypted by a first encryption method. See p. 22, line 22 - p. 23, line 1, for example.

Regarding claim 6, the Office Action asserts that the limitation which recites "generated by encrypting using a second encryption method" is indefinite as to which unit/component generates the second encrypted user name and second encrypted password. However, Applicant respectfully submits that the limitation, when read in its entirety, recites that the client apparatus includes a fourth unit which generated the encrypted user name and encrypted password.

Regarding claim 7, the Office Action asserts that the limitation reciting a predetermined method is indefinite. However, Applicant respectfully submits that the term "encrypting by a predetermined method" means encrypting predetermined information, such as any desired character string, with the unique information and also with the user name. See p. 21, lines 16-21, for example.

Regarding claim 9, the Office Action asserts that the limitations reciting a first and second encryption method are indefinite as to their scope. However, Applicant respectfully submits that one of ordinary skill in the art would recognize the scope of the term encryption. Furthermore, support for these limitations may be found in the specification. See p. 23, lines 1-5 and p. 27, line 25 - p. 28, lines 1-4, for example.

Regarding claim 9, the Office Action asserts that the limitation reciting a retention unit is indefinite as to how unique information is associated with at least one of a user name and password. Claim 9 is amended to recite that the local authentication generates unique information in response to the user's input. See p. 20, line 21 - p. 21, line 4 and Fig. 3, for example.

Regarding claim 10, the Office Action asserts that the limitation reciting a predetermined period is indefinite as to the definition of a predetermined period. However, Applicant respectfully submits that the predetermined period may be any fixed length of time. In one embodiment of the present apparatus and method, the connection only allows the client to communicate with it for a fixed period of time, such as sixty seconds. See p. 26, lines 3-16 and Fig. 4, for example.

Regarding claim 11, the Office Action asserts that the limitation reciting "wherein the client apparatus" is indefinite as to the meaning of the term first authentication information. However, Applicant respectfully submits that the first authentication information is the

unique information generated by the client apparatus, such as the serial number of the hard disk. See p. 20, lines 21-25, for example.

Regarding claim 11, the Office Action asserts that the limitation reciting "wherein the client apparatus" is indefinite as to the meaning of the term local authentication information. However, Applicant respectfully submits that the local authentication information is the first information and the second information, where the first information is the unique information encrypted with predetermined information and the second information is the user name encrypted with predetermined information. See p. 21, line 11 - p. 22, line 2, for example.

Regarding claim 11, the Office Action asserts that the limitation reciting "wherein the client apparatus" is indefinite as to the meaning of the term "predetermined information." However, Applicant respectfully submits that predetermined information may be any desired character string or may be meaningful information of the expiration date of the RAS connection, etc. See p. 21, lines 11-21, for example.

Regarding claim 11, the Office Action asserts that the limitation reciting "wherein the client apparatus" is indefinite as to the meaning of information unique to the client apparatus. However, Applicant respectfully submits that information unique to the client apparatus refers to the unique information, such as the serial number of the hard disk, which better distinguishes one client apparatus from another. See p. 20, line 22 - p. 21, line 4.

In view of the above, claims 1-3, 5-7 and 9-13 are not indefinite under 35 U.S.C. §112, second paragraph. Withdrawal of the rejection of these claims under 35 U.S.C. §112, second paragraph, is respectfully solicited.

II. Claim rejections under 35 U.S.C. §102(b) and/or §103(a)

The Advisory Action indicates that claims 1-3, 5-7 and 9-13 remain finally rejected under 35 U.S.C. §102(b) and/or 35 U.S.C. §103(a). However, the Advisory Action only

states that each of Applicant's arguments has been found non-persuasive "due to the existing broad scope of the current set of claims, reading on the primary [and secondary] reference."

Thus, the reasoning is unclear as to why the Advisory Action finds the arguments in the Amendment After Final Rejection non-persuasive and maintains the rejections under 35 U.S.C. §102(b) and/or 35 U.S.C. §103(a).

Accordingly, the remarks from the Amendment After Final Rejection are reproduced below either verbatim or with modification as follows:

- A. the remarks regarding the "seventh unit for performing an authentication process" are reproduced below verbatim;
- B. the remarks regarding the "second unit for ... transmitting the connection server address to the client apparatus" and the "receiving and transmitting unit for receiving a connection server address" are reproduced with revisions incorporating the amendments to claims 3, 6, 7, 9, 11 and 12, reciting "independent of the connection server", as discussed during the personal interview; and
- C. the remarks regarding "the connection server has shifted to a wait state" are reproduced with revisions incorporating the amendments to claims 10 and 13, reciting "wait state in which the connection server allows communication from the address of the client apparatus", as discussed during the personal interview.

The Office Action rejects claims 5 and 10 under 35 U.S.C. §102(b) and rejects claims 1, 3, and 12 under 35 U.S.C. §103(a) over Zhang et al. (U.S. 6,253,327). The Office Action further rejects claims 2, 6, 7, 9, 11 and 13 under 35 U.S.C. §103(a) over Zhang in view of Leveridge et al. (U.S. 7,233,997). These rejections are respectfully traversed.

A. Zhang does not disclose or suggest a connection server including a seventh unit for performing an authentication process

The Office Action asserts that Zhang discloses a seventh unit for performing an authentication process. However, Applicant respectfully submits that Zhang does not disclose or suggest a connection server including a seventh unit for performing an

authentication process by using the second connection authentication information transmitted from the client address, as recited in claim 1 and similarly in claim 5.

As discussed during the personal interview, Zhang discloses a gateway device that controls access to a public and private domain. See column 5, line 56 and Fig. 4. When a client sends a connection request to gateway device, the device generates and forwards to an authentication server a RADIUS account logon request packet. See column 7, lines 10-13 and Fig. 5. The gateway device must send this information to the authentication server because it itself has no authentication unit. There is nothing in Zhang which discloses or suggests a connection server including a seventh unit for performing an authentication process by using the second connection authentication information, as recited in claim 1 and similarly in claim 5. Accordingly, Zhang does not disclose or suggest the subject matter recited in claims 1 and 5.

The Office Action asserts that Leveridge discloses a message digest of the first connection authentication information. However, Leveridge does not supply the subject matter missing from Zhang. Thus, Zhang and Leveridge, individually or in combination, do not disclose or suggest the subject matter in claim 1 and similarly in claim 5.

In view of the above, Zhang and Leveridge, individually or in combination, do not disclose or suggest the subject matter recited in claims 1 and 5. Claim 2 depends from claim 1. Thus, Zhang and Leveridge, individually or in combination, do not disclose or suggest the subject matter recited in claims 1, 2 and 5. Withdrawal of the rejection of these claims under 35 U.S.C. §102(b) and/or 35 U.S.C. §103(a) is respectfully solicited.

B.1. Zhang does not disclose a second unit for ... transmitting, independent of the connection server, the connection server address to the client apparatus

Regarding claims 3, 6 and 7, the Office Action admits that Zhang does not disclose a second unit for ... transmitting the connection server address to the client apparatus, as recited in claim 3 and similarly in claims 6 and 7. The Office Action asserts, however, that it would have been obvious to one of ordinary skill in the art to include this limitation since it is implied that the address of each communicating device is sent with each communication. See p. 17-18. However, Applicant respectfully submits that Zhang does not disclose or suggest the authentication server transmitting, independent of the connection server, the connection server address to the client apparatus because the authentication server in Zhang never communicates with the host. See Figs. 1, 2 and 4, for example. There is nothing in all of Zhang that discloses or suggests a second unit for ... transmitting, independent of the connection server, the connection server address to the client apparatus, as recited in claim 3 and similarly in claims 6 and 7. Thus, Zhang does disclose or suggest the subject matter recited in claim 3, and similarly in claims 6 and 7.

The Office Action asserts that Leveridge discloses a message digest of the first connection authentication information. However, Leveridge does not supply the subject matter missing from Zhang. Thus, Zhang and Leveridge, individually or in combination, do not disclose or suggest the subject matter in claim 3 and similarly in claims 6 and 7.

In view of the above, Zhang and Leveridge, individually or in combination, do not disclose or suggest the subject matter recited in claims 3, 6 and 7. Withdrawal of the rejection of these claims under 35 U.S.C. §102(b) and/or 35 U.S.C. §103(a) is respectfully solicited.

B.2. Zhang does not disclose a receiving and transmitting unit for receiving, independent of the connection server, a connection server address from the authentication server

Regarding claims 9, 11 and 12, the Office Action asserts that Zhang discloses or suggests a receiving and transmitting unit for receiving a connection server address from the authentication server, as recited in claim 9 and similarly in claims 11 and 12. However, Applicant respectfully submits that Zhang does not disclose a receiving and transmitting unit for receiving, independent of the connection server, a connection server address from the authentication server.

As explained earlier in the Amendment, Zhang does not disclose that the authentication server ever communicates with the host. See Figs. 1, 2 and 4, for example. Thus, even if the authentication server were to include its own address in its communications with other devices, it would never send the address of a connecting server to the client apparatus. There is nothing in all of Zhang that discloses or suggests a receiving and transmitting unit for receiving, independent of the connection server, a connection server address from the authentication server, as recited in claim 9 and similarly in claims 11 and 12. Accordingly, Zhang does not disclose or suggest the subject matter recited in claim 9 and similarly in claims 11 and 12.

The Office Action asserts that Leveridge discloses a message digest of the first connection authentication information. However, Leveridge does not supply the subject matter missing from Zhang. Thus, Zhang and Leveridge, individually or in combination, do not disclose or suggest the subject matter in claims 9, 11 and 12.

In view of the above, Zhang and Leveridge, individually or in combination, do not disclose or suggest the subject matter recited in claims 9 and 11. Withdrawal of the rejection of these claims under 35 U.S.C. §102(b) and/or 35 U.S.C. §103(a) is respectfully solicited.

C. Zhang does not disclose or suggest a transmitting unit that transmits to the authentication server information indicating that the connection server has shifted to a wait state

Regarding claims 10 and 13, the Office Action asserts that Zhang discloses or suggests a transmitting unit that transmits to the authentication server information indicating that the connection server has shifted to a connection wait state. As discussed during the personal interview, claims 10 and 13 are amended for the purpose of clarity to recite a "wait state in which the connection server allows communication from the address of the client apparatus".

Furthermore, Applicant respectfully submits that Zhang does not disclose or suggest a transmitting unit that transmits to the authentication server information indicating that the connection server has shifted to a wait state, as recited in claim 10 and similarly in claim 13.

Zhang discloses that if the authentication process was unsuccessful then the gateway device sends a prompt back to the host notifying the subscriber. See column 7, lines 25-29. This message is sent to the host and not to the authentication server. There is nothing in all of Zhang that discloses or suggests a transmitting unit that transmits to the authentication server information indicating that the connection server has shifted to a wait state, as recited in claim 10 and similarly in claim 13. Accordingly, Zhang does not disclose or suggest the subject matter of claims 10 and 13.

The Office Action asserts that Leveridge discloses a message digest of the first connection authentication information. However, Leveridge does not supply the subject matter missing from Zhang. Thus, Zhang and Leveridge, individually or in combination, do not disclose or suggest the subject matter in claims 10 and 13.

In view of the above, Zhang and Leveridge, individually or in combination, do not disclose or suggest the subject matter recited in claims 10 and 13. Withdrawal of the rejection of these claims under 35 U.S.C. §102(b) and/or 35 U.S.C. §103(a) is respectfully solicited.

In view of the foregoing, it is respectfully submitted that this application is in condition for allowance. Favorable consideration and prompt allowance of claims 1-3, 5-7 and 9-13 are earnestly solicited.

Should the Examiner believe that anything further would be desirable in order to place this application in even better condition for allowance, the Examiner is invited to contact the undersigned at the telephone number set forth below.

Respectfully submitted,



James A. Oliff
Registration No. 27,075

Kipman T. Werking
Registration No. 60,187

JAO:KTW/eks

Attachments:

Petition for Extension of Time
Request for Continued Examination

Date: January 22, 2008

OLIFF & BERRIDGE, PLC
P.O. Box 320850
Alexandria, Virginia 22320-4850
Telephone: (703) 836-6400

<p>DEPOSIT ACCOUNT USE AUTHORIZATION Please grant any extension necessary for entry; Charge any fee due to our Deposit Account No. 15-0461</p>
